LAPORAN AKHIR

PROYEK

SQL SERVER SECURITY

DisusunOleh:

Nama : 11117320

NPM : Chantika Amanda

Kelas :

LEMBAGA PENGEMBANGAN KOMPUTERISASI

UNIVERSITAS GUNADARMA

2022

DAFTAR ISI

DESKRIPSI LAPORAN

SQL SERVER SECURITY

Pada pertemuan 5 laporan berisikan mengenai Security Principals dan Securables di SQL Server, memahami Mode otentikasi di SQL Server, memahami users dan logins di SQL Server, dapat menerapkan password policy, dan mencegah SQL Injection

TAHAPAN PENGERJAAN

1. RingkasanMateri

Entitas yang dapat meminta/ memiliki akses ke server, database, atau schema disebut sebagai security principals. Sedangkan item yang dapat diamankan untuk mengontrol akses terhadap item tersebut disebut securables. Security principals dapat digolongkan menjadi 2 kelompok yaitu:

- Indivisible principals adalah sebuah entitas yang tidak bergantung terhadap entitas lainnya. Contohnya yaitu SQL login dan Windows login.
- Collection principals adalah principal yang merepresentasikan sekelompok entitas yang diperlakukan sebagai sebuah kesatuan. Contoh dari principal ini yaitu Windows group.

Terdapat tiga level keamanan yang dapat diolah pada security principals SQL Server, yaitu Windows, SQL Server, dan database. Pada masing-masing level terdapat lagi security principals yang dapat diolah. Berikut ini principals yang terdapat pada masing-masing tingkatan.

- Windows level principals
  - Domain logins
  - Local system logins
- SQL Server level principals
  - SQL Server login
  - Windows login
- Database level principals
  - Users
  - Roles
  - Applicaition roles

Securables adalah semua resources dalam SQL Server yang dapat diatur hak aksesnya. Contoh securable yaitu sebuah tabel. Terdapat tiga tingkat cakupan dari securables yaitu server, database, dan schema. Berikut ini securables pada masing-masing tingkatan.

- Server
  - SQL Server instance
  - Endpoint
  - Login
  - Server role
  - Database
- Database
  - Application role

    - Assembly
    - Asymmetric key
    - Certificate
    - Contract
    - Fulltext catalog
    - Fulltextstoplist
    - Message type
    - Remote Service Binding
    - (Database) Role
    - Route
    - Schema
    - Search property list
    - Service
    - Symmetric key
    - User
- Schema
    - Type
    - XML schema collection
    - Object. Berikut ini yang termasuk ke dalam object pada schema:
        - Aggregate
        - Function
        - Procedure
        - Queue
        - Synonym
        - Table
        - View
        - External Table

Terdapat dua macam mode otentikasi pada SQL Server yaitu:

- Mode otentikasi Windows: Penggunaan mode ini paling cocok ketika database hanya diakses dalam satu lingkup organisasi.
- Mode otentikasi SQL Server dan Windows (mixed mode): Penggunaan mode ini paling cocok ketika database juga diakses oleh pengguna yang berada di luar lingkup suatu organisasi (diluar domain Windows) atau pun pengguna yang tidak menggunakan perangkat Windows.

Dengan menggunakan mode otentikasi Windows, pengguna dapat login ke SQL Server baik dengan menggunakan user account maupun group acccount. Mode otentikasi Windows ini lebih memudah user untuk masuk ke dalam SQL Server karena user tidak perlu untuk mengingat username SQL Server login dan password- nya.

Dengan keamanan campuran (mixed security), pengguna menggunakan otentikasi Windows dan login SQL Server. Login SQL Server terutama untuk pengguna di luar perusahaan, seperti mereka yang mungkin mengakses database dari Internet. Anda dapat

mengkonfigurasi aplikasi yang mengakses SQL Server dari Page 5 Internet untuk menggunakan akun tertentu secara otomatis atau untuk meminta pengguna memasukkan ID masuk dan kata sandi SQL Server.

Sebagaimana yang telah dibahas sebelumnya bahwa SQL Server memiliki 2 metode otentikasi yang berarti terdapat 2 jenis login server. Pengguna bisa login Windowsdengan menggunakan domain account atau local account, local group account atau universal dan global domain group account. Pengguna bisa juga menggunakan login SQL Server dengan menentukan ID login dan password yang unik. Beberapa login dikonfigurasi secara default, yaitu local Administrators, local Administrator,sa. Penggunaan user untuk mempersempit ruang lingkup akses ke database. Beberapa users dikonfigurasi secara default, termasuk the dbo user, dan the guest user

Administrators Group

Administrators group adalah sebuah grup lokal dalam server database. Anggota dari grup ini biasanya akun local Administrator user dan user lainnya yang telah diatur sebagai administrator dalam lokal sistem. Di SQL Server, grup ini diberikan hak akses sebagai sysadmin server role secara default.

Administrator User Account

Administrator adalah sebuah user account lokal di server. Akun ini memberikan hak akses sebagai administrator pada sistem. Jika SQL Server terpasang di Windows domain, maka administrator account biasanya memiliki hak akses secara domain juga. Pada SQL Server, akun ini mendapatkan hak akses sysadmin server role secara default.

Sa Login

Sa login adalah aku sistem administrator si SQL Server. Dengan model keamanan baru yang telah terintegrasi dan diperluas, sa tidak lagi dibutuhkan. Sa disediakan untuk kompabilitas terhadap SQL Server versi sebelumnya. Seperti login administrator lainnya, sa diberikan server sysadmin role secara default. Saat Anda menginstal SQL Server, login sa tidak diberi kata sandi. Untuk mencegah akses yang tidak sah ke server, kata sandi harus benar-benar kuat, dan harus diganti secara berkala.

Guest User

Guest User adalah pengguna khusus yang dapat Anda tambahkan ke database untuk memungkinkan seseorang dengan login SQL Server yang valid untuk mengakses database. Pengguna yang mengakses database dengan guest account menganggap identitas pengguna tamu dan mewarisi semua hak istimewa dan hak akses akun tamu. Misalnya, jika Anda mengonfigurasi akun GOTEAM untuk mengakses SQL Server, GOTEAM dapat mengakses database apa pun dengan info masuk tamu, dan saat GOTEAM melakukannya, orang yang masuk di bawah GOTEAM diberikan semua hak akses akun tamu. Jika Anda mengkonfigurasi grup Windows DEVGROUP dengan akses tamu, Anda dapat menyederhanakan administrasi karena setiap pengguna yang merupakan anggota grup akan

dapat mengakses database apa pun sebagai tamu. Guest user adalah user khusus yang dapat ditambahkan ke database untuk memungkinkan seseorang dengan login SQL Server yang valid untuk mengakses database. User yang mengakses database dengan guest account mewarisi semua privillages dan permission yang dimiliki oleh guest user. Secara default, guest user terdapat di database model. Karena database model adalah template untuk semua database yang dibuat, semua database baru memiliki guest user. Guest user tidak dapat dihapus namun bisa dinonaktifkan kecuali pada database master dan tempdb. Hal ini tidak menjadi masalah karena guest user memiliki privillage dan permission yang terbatas di database tersebut.

2. Langkah-Langkah

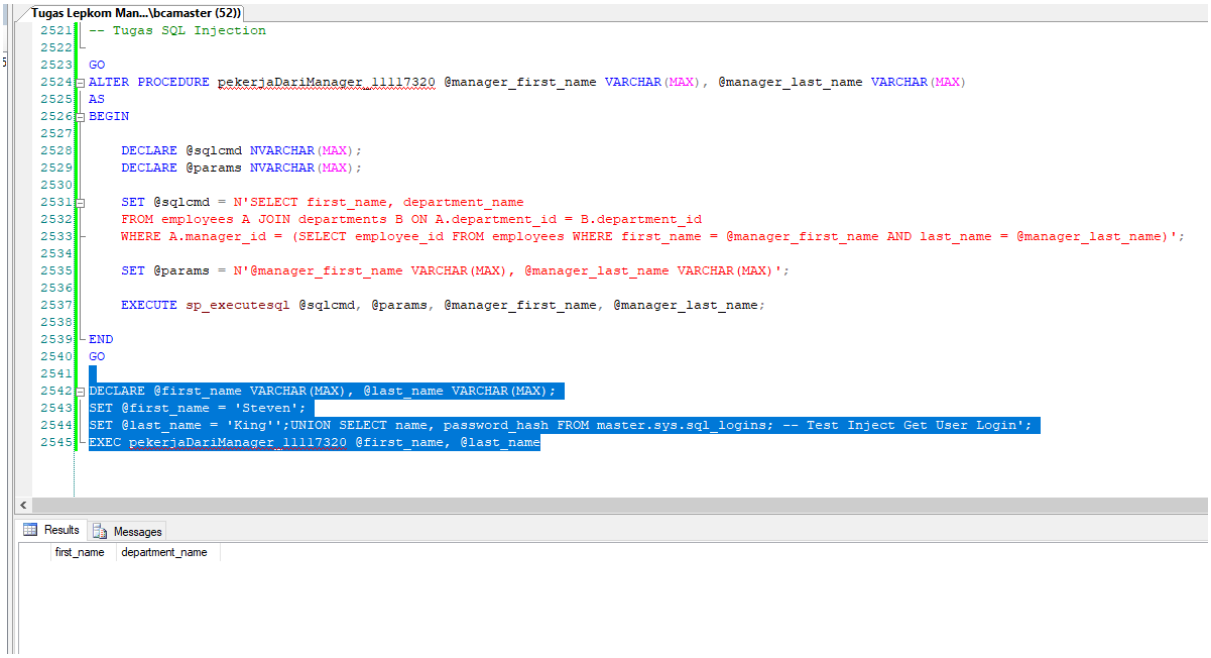
1. **Manakah mode otentikasi yang lebih baik antara mode Windows dan mode campuran? Sertakan alasannya!**

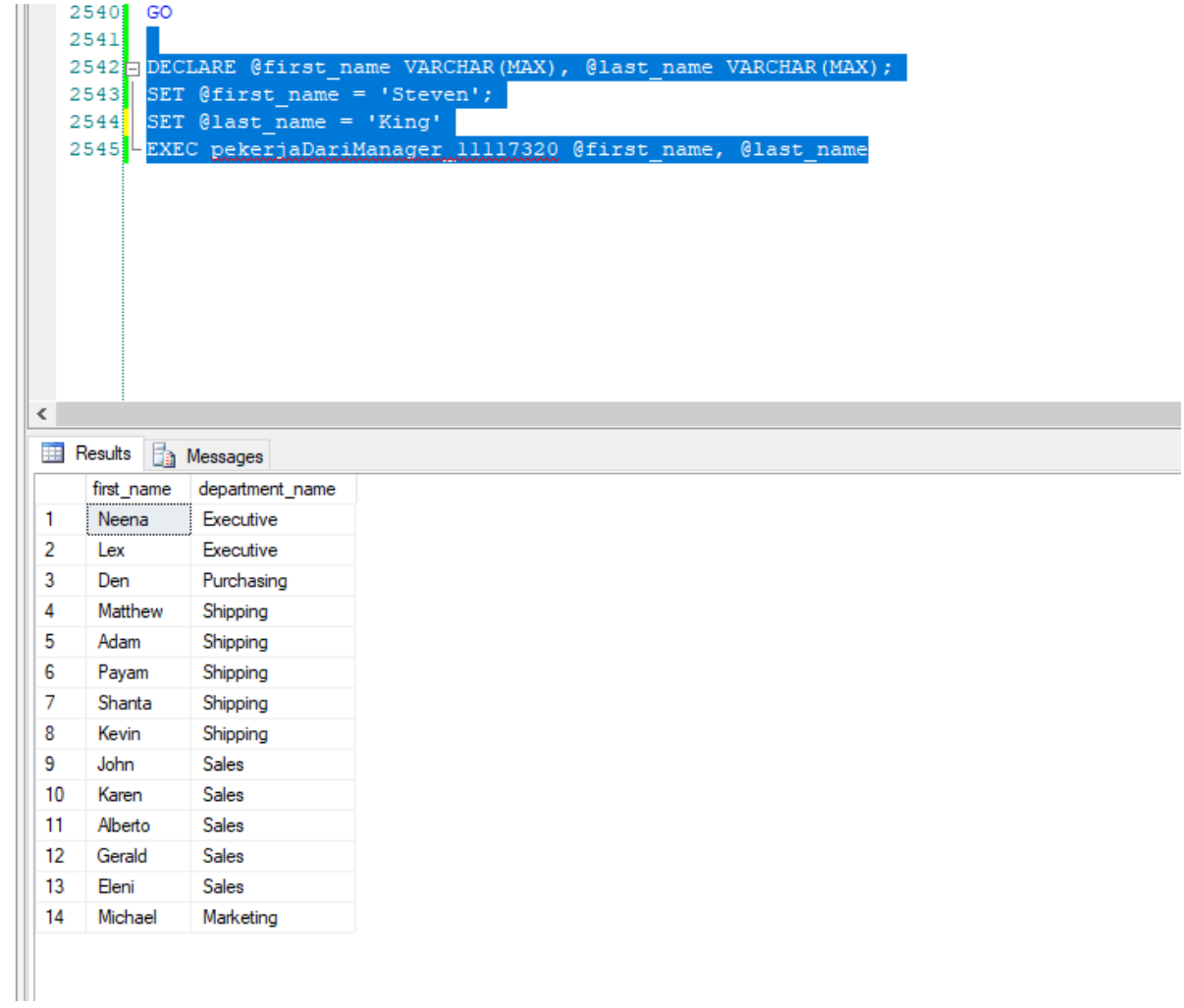
   Mode otentikasi Campuran lebih baik karena Penggunaan mode ini dapat digunakan ketika database juga diakses oleh pengguna yang berada di luar lingkup suatu organisasi (diluar domain Windows) atau pun pengguna yang tidak menggunakan perangkat Windows Selain itu Anda dapat mengkonfigurasi aplikasi yang mengakses SQL Server dari Page 5 Internet untuk menggunakan akun tertentu secara otomatis atau untuk meminta pengguna memasukkan ID masuk dan kata sandi SQL Server

2. **Buatlah password policy untuk perusahaan x pada Local/Domain Security Policy, berikan alasan yang konkrit untuk masing-masing kebijakan/policy yang telah Anda tentukan**

   Kebijakan yang akan dibuat yaitu "*enforce password history* = 12" sehingga dalam 1 tahun tidak ada password yang berulang selanjutnya "*maximum password age* = 30" yang artinya setiap 1 bulan sekali user harus melakukan perubahan password selanjutnya "*minimum password age* = 15" ini artinya password yang baru diganti tidak dapat diganti lagi dalam waktu < 15 hari selanjutnya "*minimum password length* = 9" sehingga minimal jumlah karakter untuk suatu password yaitu 9 character dengan mengikuti aturan "*Password must meet complexity requirements"* default

3. **SQL Injection (**Dengan menggunakan sp_executesql dan param maka kita telah berhasil mencegah SQL Injection yang mencoba menampilkan seluruh user Login pada Instance yang sedang di Hit, selain itu fungsi dari Procedure masih berjalan baik dan dapat dilihat pada Gambar kedua)





	first_name	department_name
1	Neena	Executive
2	Lex	Executive
3	Den	Purchasing
4	Matthew	Shipping
5	Adam	Shipping
6	Payam	Shipping
7	Shanta	Shipping
8	Kevin	Shipping
9	John	Sales
10	Karen	Sales
11	Alberto	Sales
12	Gerald	Sales
13	Eleni	Sales
14	Michael	Marketing

PENUTUP

1. Kesimpulan

Pada Praktikum ini telah mempelajari mengenai Security Principal pada SQL Server, memahami mengenai Metode Otentikasi Kelebihan dan Kekurangannya, memahami mengenai ap aitu SQL Injection dan bagaimana cara mencegahnya, memahami Users dan Login pada SQL Server dan menrapkan Password Policy

2. SaranPenulisan